Ausfallsicherheit bei Cyberangriffen – Erkenntnisse

Zu Lücken bei der Ausfallsicherheit bei Cyberangriffen, sich entwickelnden Bedrohungen, KI-gesteuerten Abwehrmaßnahmen und Recovery-Strategien in APJ

Die Herausforderungen im Bereich der Ausfallsicherheit bei Cyberangriffen nehmen zu, da Cyberangriffe und Lücken im Datenschutz das Risiko von Störungen erhöhen. Unternehmen mit ausgereiften Strategien* zur Ausfallsicherheit bei Cyberangriffen sind nahezu dreimal häufiger in der Lage, Cyberangriffe erfolgreich zu überstehen. Durch die Modernisierung von Resilienzstrategien, den Ausbau von Erkennungsfunktionen und die Priorisierung kontinuierlicher Optimierung können IT-Führungskräfte Risiken minimieren und das Vertrauen in ihre Fähigkeit stärken, sich an sich weiterentwickelnde Bedrohungen anzupassen.

Übermäßiger Optimismus bei Führungskräften

74 % der IT-Fachkräfte sind der Ansicht, dass ihre Führungsebene die Bereitschaft für Cybervorfälle überschätzt. Bei zu viel Optimismus entstehen gefährliche blinde Flecken, durch die sich kritische Investitionen verzögern und Schwachstellen offen bleiben.

Die Lücke zwischen Selbstbewusstsein und Funktionalitäten

99,3 % der Unternehmen verfügen über Strategien zur Ausfallsicherheit bei Cyberangriffen

Und **55 %** konnten keine effektive Recovery nach dem letzten Test oder Incident durchführen

Prävention vs. Recovery: ein unausgewogener Ansatz

87 % glauben, dass sich ihr Unternehmen mehr auf die Verhinderung von Angriffen als auf Vorbereitungen für die Wiederherstellung nach einem Angriff konzentriert

Jedoch nur **30 %** verfügen über eine umfassende Plattform für die Bedrohungserkennung sowohl im primären Storage als auch im Backup-Storage und der Netzwerkinfrastruktur

Und nur **41 %** gelang Eindämmung und Recovery nach einem Angriff oder Cyber-Incident-Drill mit minimalen Auswirkungen

Folglich sind viele Organisationen nicht auf die Recovery-Phase vorbereitet, die über das Überleben des Unternehmens entscheidet, wenn Sicherheitsverletzungen unvermeidlich auftreten.

Der Weg in die Zukunft:
Ausgereifte Unternehmen liefern Ergebnisse

Unternehmen mit ausgereiften Strategien zur Ausfallsicherheit bei Cyberangriffen sind nahezu 2,8-mal häufiger in der Lage, Cyberangriffe erfolgreich zu überstehen

Bei strategischer Reife in drei wesentlichen Bereichen entsteht unerschütterliche Resilienz.

SICHERHEIT:
Aufbau Ihrer Vertrauensgrundlage

Unternehmen mit einer ausgereiften Strategie für die Ausfallsicherheit bei Cyberangriffen:

- **schützen Geräte 1,8-mal** wahrscheinlicher mithilfe von Sicherheitskontrollen auf Firmware-/BIOS-Ebene
- **nutzen mit höherer Wahrscheinlichkeit** Verschlüsselung für Data at Rest und für Data in Transit
- **nutzen mit höherer Wahrscheinlichkeit** Cyber Vaults, um kritische Daten vor sich weiterentwickelnden Bedrohungen zu schützen

Aber Sicherheit ist nur der Anfang. Einen echten Vorteil verschaffen Sie sich durch intelligente Erkennung, die Bedrohungen bemerkt, bevor sie Ihre wertvollsten Ressourcen gefährden.

ERKENNUNG:
Permanent aktive Intelligenz

Die Herausforderung der Sichtbarkeit:
Nur 30 % der Unternehmen verfügen über eine robuste Bedrohungserkennung für Backup-Storage, primären Daten-Storage und Netzwerkinfrastruktur

Die KI-gestützte Lösung:

- **57 %** priorisieren Investitionen in KI-/ML-gestützte Bedrohungserkennung
- **52 %** scannen Backupdaten umfassend mit KI/ML auf Indikatoren für eine Gefährdung
- Organisationen mit ausgereiften Strategien nutzen mit **2,3-mal höherer Wahrscheinlichkeit** KI-/ML-Tools mit proaktiven Playbooks zur Minderung und Reaktion

RECOVERY:
Wo Vorbereitung auf Performance trifft

Der Testvorteil:

- **61 %** der Unternehmen, die monatlich oder häufiger Cyberangriffe simulieren, waren mit der Recovery nach Vorfällen erfolgreich
- **59 %** der Unternehmen, die weniger als einmal im Monat Tests durchführen, konnten keine erfolgreiche Recovery nach Vorfällen vorweisen

Ergebnis:
Unternehmen, die häufig testen, erfüllen deutlich häufiger sowohl die Recovery Time Objectives (RTO) als auch die Recovery Point Objectives (RPO) als diejenigen, die nur sporadisch testen.

Ihr Weg zu hervorragender Ausfallsicherheit bei Cyberangriffen

Unternehmen mit einer ausgereiften Strategie für Ausfallsicherheit bei Cyberangriffen sind mit 2,3-facher Wahrscheinlichkeit in der Lage, ihre SLAs konsistent einzuhalten

Aufbau einer robusten Grundlage
Priorisieren Sie sowohl Prävention als auch schnelle Recovery.

- **Sicherheit:** Reduzieren Sie Risiken mit Sicherheitskontrollen auf BIOS-Ebene, Datenverschlüsselung und Cyber-Vaults für kritische Daten.
- **Erkennung:** Nutzen Sie KI/ML in Echtzeit, um Bedrohungen im gesamten Storage zu erkennen und darauf zu reagieren, einschließlich primärem Storage und Protection-Storage.
- **Recovery:** Testen Sie die Recovery häufig. Unternehmen, die dies monatlich tun, erreichen die Recovery-Ziele viel häufiger.

Bereit für mehr Ausfallsicherheit bei Cyberangriffen?

Bereit für mehr Ausfallsicherheit bei Cyberangriffen? Lesen Sie die wichtigsten Erkenntnisse aus der *Studie Cyber Resilience Insights 2026 von Dell.*

DELL Technologies

Quelle: Vanson Bourne und Dell Technologies Umfrage zur Ausfallsicherheit bei Cyberangriffen 2025.

* Als Unternehmen mit ausgereiften Strategien für Ausfallsicherheit bei Cyberangriffen werden solche definiert, deren Strategie durchgängig eingesetzt und kontinuierlich optimiert wird. Dafür werden voraussichtlich Analysen, Automatisierung und Echtzeitmetriken (z. B. Threat-Intelligence-Feeds, ML-gestützte Anpassungen, KPIs zur Steuerung von Verbesserungen) eingesetzt.